The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):

http://www.fiscal.treasury.gov/fsreports/fspia/fs_pia.htm

Name of Service: Non-Traditional Alternative Payments (NTAP) Pilot

Document Version: 2.1

Document Date: January 7, 2015

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

As a strategic priority within Payment Management to reduce the number of paper checks disbursed, the NTAP Pilot provides Federal agencies another electronic alternative to the Go Direct and Direct Express Programs. The NTAP process seeks to pilot an E-wallet solution by generating payments to Federal employees via existing Networks such as ClearXchange, Google Wallet, PayPal, PopMoney, SquareCash, and Venmo among others that may be added. These established networks utilize an email address or cell phone number to initiate a payment and utilizes existing commercial payments ACH and debit card infrastructure.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

FMS .002 Payment Records

3) If the system is being modified, will the SORN require amendment or revision?
__yes, explain.
_X_ no

4) Does this system contain any personal information about individuals?
_X_ yes
___no

a. Is the information about members of the public? No

b. Is the information about employees or contractors? Yes – Federal Employees

5) What legal authority authorizes the purchase or development of this system?
31 CFR 208 DCIA

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:
_X_ Employees
__ Contractors
__ Taxpayers
__ Others (describe)

2) **Identify the sources of information in the system**
Check all that apply:

_ _ Employee
__ Public
_X_ Federal agencies
__ State and local agencies
__ Third party

a. What information will be collected from employees or contractors?
The service will contain work Email addresses, work provided blackberry phone numbers, and debit card or bank account number.

b. What information will be collected from the public?
None

c. What Federal agencies are providing data for use in the system?
Department of Justice; US Marshal Service

d. What state and local agencies are providing data for use in the system?
None

e. From what other third party sources will data be collected?
None

3) **Accuracy, Timeliness, and Reliability**

a. How will data collected from sources, other than Fiscal Service records, be verified for accuracy?
Payment data comes only from a Federal Program Agency (FPA). The FPA responsible for sending the data is responsible for the accuracy of the payment data submitted.

b. How will data be checked for completeness?
The FPA certifies data for completeness.

c. What steps or procedures are taken to ensure the data is current?
The FPA certifies data for completeness.

d. In what document(s) are the data elements described in detail?
Data elements are described in design documents.

ATTRIBUTES OF THE DATA:

1) **How is the use of the data both relevant and necessary to the purpose for which the system is being designed?**
   The data is relevant and necessary for the proper processing of payments from the FPA. Work Email addresses, work provided blackberry phone numbers, and debit card or bank account number are key components of an E-Wallet solution.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?**
   No

3) **Will the new data be placed in the individual's record?**
   No

4) **Can the system make determinations about employees or members of the public that would not be possible without the new data?**
   No

5) **How will the new data be verified for relevance and accuracy?**
   N/A

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**
   All data collected in the NTAP Pilot is protected utilizing strong encryption methods.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**
   Yes, see #6 above

8) **How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)**
   Through industry standard and enterprise grade authenticated, dual account, group policy and access control methods. Work Email addresses, work provided blackberry phone numbers, and debit card or bank account number are used to identify payees.

9) **What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
   None

10) **What opportunities do individuals have to decline to provide information (i.e., in such cases where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)? How can individuals grant consent?**
   Participation is voluntary.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **What are the retention periods of data in this system? How long will the reports produced be kept?**
   Data is kept based on the standard retention policy unless a different interval is required by customer.

2) **What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?**
   Industry best practices for data base rescission and complete removal from system disk

3) **If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?**
   Although replication is used for uptime and QOS, cloud based implementation is technically distributed but it's logically in "one" place.

4) **Is the system using technologies in ways that Fiscal Service has not previously Employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
   Yes

5) **How does the use of this technology affect employee or public privacy?**
   Not applicable

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
   No.

7) **What kind of information is collected as a function of the monitoring of individuals?**
   None.

8) **What controls will be used to prevent unauthorized monitoring?**
   Industry best practices for firewalling; perimeter protection and system monitoring are employed. Users are required to sign Rules of Behavior (ROB) and 3rd party vendors are required to sign Non-Disclosure Agreements (NDA). Periodic reviews will be performed to prevent unauthorized monitoring.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   - **_X_ Contractors**
   - **__ Users**
   - **_X_ Managers (Certifying Officer)**
   - **_X_ System Administrators**
   - **_X_ System Developers**
   - **_X_ Others (explain) -** Treasury authorized users to verify and certify payment.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
Criteria, procedures, and controls are documented.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**
Yes - User access will be restricted to specific roles and responsibilities.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**
See #2 & #3

5) **If contractors are/will be involved with the design, development or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?**
Yes

6) **Do other systems share data or have access to the data in the system?**
__yes
_X_no

If yes,

a. Explain the interface. N/A

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface. N/A

7) **Will other agencies share data or have access to the data in this system?**
__yes
_X_no

If yes,

a. Check all that apply:
__Federal
__State
__ Local
__Other (explain) _____

b. Explain how the data will be used by the other agencies.

c. Identify the role responsible for assuring proper use of the data.